

IN THE UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF MISSOURI  
EASTERN DIVISION

MONSANTO COMPANY,	)	
	)	
and	)	
	)	
THE CLIMATE CORPORATION,	)	
	)	
Plaintiffs,	)	
	)	
v.	)	Case No. 4:16-cv-876
	)	
JIUNN-REN CHEN,	)	
	)	
and	)	
	)	
JOHN AND JANE DOES 1 THROUGH	)	
10 AND OTHER JOHN DOE	)	
CORPORATIONS 1 THROUGH 10	)	
	)	
Defendants.	)	

**COMPLAINT**

Plaintiffs, Monsanto Company and The Climate Corporation, file this action against Jiunn-Ren Chen (“Defendant”) seeking relief under the Defend Trade Secrets Act of 2016 (18 U.S.C. § 1836(b)(1), as amended), and allege as follows:

**THE PARTIES**

1. Monsanto Company is a company organized and existing under the laws of the State of Delaware with its principal place of business in St. Louis, Missouri.
2. The Climate Corporation is a wholly-owned subsidiary of Monsanto Company, with its principal place of business in San Francisco, California.
3. Jiunn-Ren Chen, also known as J.R. Chen, is, upon information and belief, a resident of the state of Missouri.

## **JURISDICTION AND VENUE**

4. The Court has subject matter jurisdiction in this matter pursuant to 28 U.S.C. § 1331 as the Defend Trade Secrets Act of 2016, 18 U.S.C. § 1836, as amended, provides federal courts with subject matter jurisdiction over civil actions based on the misappropriation of trade secrets.

5. Venue is appropriate in this judicial district under 28 U.S.C. §1391(b)(1) because Defendant resides within this judicial district. Venue is also appropriate under 28 U.S.C. §1391(b)(2) because a substantial part of the events or omissions giving rise to the claims herein occurred and/or a substantial part of the property that is the subject of this action is situated within this judicial district.

## **FACTS**

6. Jiunn-Ren Chen was employed as a data science analyst by Monsanto Company, and also performed work for The Climate Corporation, a wholly-owned subsidiary of Monsanto Company.

7. The Climate Corporation helps the world's farmers sustainably increase their productivity with digital tools.

8. The Climate Corporation uses proprietary algorithms and predictive analytics to enhance technological tools sold to farmers. As such, confidential trade secrets are of vital importance and substantial value to Plaintiffs' current and future business interests.

9. In his capacity as a data science analyst, Mr. Chen wrote code and/or algorithms that were of vital importance to Plaintiffs.

10. As part of his work for Plaintiffs in performing these duties, Mr. Chen helped create and thus had access to Plaintiffs' confidential trade secrets and proprietary information.

11. Mr. Chen had access to this information through both a PC computer issued to him by Monsanto and a Macintosh computer issued to him by The Climate Corporation.

12. Mr. Chen, as with other Monsanto employees, was assigned unique login credentials that allowed him to enter a secure electronic environment where he created, accessed, and collaborated in the production of critical proprietary information.

13. Ordinarily, within this secure electronic environment, Plaintiffs may monitor and track all activity associated with this proprietary information.

**Plaintiffs' Discovery of Unauthorized Software**

14. On Wednesday, June 1, 2016, Mr. Chen announced that he was resigning his position with Monsanto for the stated reason that he was going to return to Taiwan in order to care for his ailing father and take over the family business in Taiwan.

15. Subsequently, Mr. Chen has admitted that in fact he has received and is considering an offer to serve as Director of Resource Management and Bioinformatics for a seed company in the People's Republic of China.

16. On June 1, 2016, the day he announced his resignation, Mr. Chen turned in his computers to Plaintiffs, inconsistent with Company practice.

17. Although his job was highly computer-dependent and his last day of work was anticipated to be June 14, 2016, Mr. Chen chose to relinquish his computers at the end of the work day on June 1, 2016.

18. Due to Mr. Chen's position with the company, Plaintiffs' IT personnel performed a standard review of these computers, and it was discovered that the computers were loaded with highly sophisticated and unauthorized software that could be used to perform reconnaissance, exfiltrate data, and conceal activity on the device.

19. Because of the existence of these unauthorized software programs, the IT department alerted the Director of Business Conduct, who then scheduled an interview with Mr. Chen to inquire about the presence of the software on the machines.

20. On Thursday, June 9, 2016, Mr. Chen was interviewed regarding this unauthorized software.

21. In his interview, Mr. Chen denied knowing the software was present on his computers.

22. In addition, Mr. Chen produced at his interviews although he was aware of other software on his machines four different data drives that he stated he had connected to his computers issued to him by Plaintiffs.

23. Mr. Chen stated that he brought these drives to the interview because he “had nothing to hide.”

24. However, Mr. Chen was then asked to provide the devices for forensic review, and Mr. Chen refused and referred Plaintiffs to his wife, who also refused permission to relinquish these data drives to Plaintiffs.

**Plaintiffs’ Discovery of Trade Secret Theft**

25. After the interview on June 9, 2016, Plaintiffs continued to monitor activity surrounding Mr. Chen’s credentials because of the unauthorized software on the company computers and Mr. Chen’s suspicious behavior.

26. The credentials themselves that had been assigned to Mr. Chen remained active at this point, but he should not have been accessible for the purpose of downloading because the only two computers authorized to perform such downloads from the Company’s secure environment had been relinquished by Mr. Chen on June 1, 2016.

27. In the course of this continued monitoring, it was documented that at 3:47 a.m. on Friday, June 10, 2016, fifty-two files were removed from Plaintiffs' secure environment through the unique account access credentials assigned to Mr. Chen.

28. As stated, because Mr. Chen had relinquished the two company computers, no download of data should have been possible using his unique credentials.

29. Plaintiffs have carefully reviewed the listing of these files and their content.

30. Plaintiffs have confirmed that the files taken at 3:47 a.m. on Friday, June 10, 2016, contained proprietary material important to Plaintiffs' current and future business.

31. The knowledge or access of these files outside of Plaintiffs' secure electronic environment, particularly by a business competitor, is of great concern to Plaintiffs and would cause them irreparable harm.

**Mr. Chen's Inculpatory Statements to Plaintiffs**

32. On Tuesday, June 14, 2016, Mr. Chen was scheduled for a routine exit interview.

33. Following this routine exit interview, Monsanto Director of Business Conduct interviewed Mr. Chen about the fifty-two files that had been removed from the secure environment through the account access credentials assigned to Mr. Chen.

34. During this interview with the Director of Business Conduct, Mr. Chen's demeanor changed noticeably and he made several inculpatory statements.

35. First, without in advance knowing the specifics of the intended basis for questioning, Mr. Chen remarked "did you find files moving."

36. Mr. Chen denied having accessed these files but, critically, he confirmed that no one else had knowledge of the unique account access credentials assigned to him.

37. Mr. Chen stated his belief that this had been done by a hacker.

38. In addition, Mr. Chen contradicted his statement from June 1, 2016, regarding the reasons for his resignation, and acknowledged that he was seeking employment in the agriculture sector in China.

39. Mr. Chen subsequently sent Monsanto unsolicited information that he has in fact received, and is considering, an offer to serve as Director of Resource Management and Bioinformatics for this company in Wuhan, China.

40. Mr. Chen also offered that he had been in contact with Mo Hailong, a Chinese national who recently pleaded to conspiracy to commit theft of trade secrets in *United States v. Hailong*, Case No. 4:13-cr-147 in the United States District Court for the Southern District of Iowa.

41. Contact between Mr. Chen and Mo Hailong occurred during the time Mo Hailong was known to be acquiring Monsanto proprietary germplasm through unauthorized means.

42. Plaintiffs believe that the conduct for which Mr. Hailong pleaded guilty could not have been achieved absent access to inside information.

43. Mr. Chen also made statements as to the degree of contact with Mo Hailong that Plaintiffs know to be untrue.

44. Mr. Chen also admitted that in travel to the People's Republic of China on previous occasions, Mr. Chen had learned and was familiar with VPN software used to cloak his online identity used to circumvent internet access controls by the Chinese government.

45. These admitted practices demonstrate the proficiency needed to accomplish the theft of trade secrets as occurred on June 10, 2016.

46. When presented with a listing of the fifty-two files that were transferred under his unique credentials, Mr. Chen acknowledged that all files contained trade secret information.

**COUNT I:  
MISAPPROPRIATION OF TRADE SECRETS  
UNDER THE DEFEND TRADE SECRETS ACT OF 2016**

47. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 46 as if fully alleged herein.

48. On May 11, 2016, President Obama signed the Defend Trade Secrets Act of 2016 (“DTSA”), which went into effect that day. The DTSA was an amendment to the Economic Espionage Act (“EEA”), 18 U.S.C. § 1831, et seq., which was enacted in 1996.

49. The DTSA provides as follows:

An owner of a trade secret that is misappropriated may bring a civil action [in federal court] under this subsection if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce. *Id.*

50. The DTSA retained the definition of “trade secrets” under the original EEA, which generally follows the Uniform Trade Secrets Act.

51. Under this definition, the term “trade secrets” covers “all forms and types of” information, regardless of how it is stored, where: “the owner thereof has taken reasonable measures to keep such information secret; and “the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by another person who can obtain economic value from the disclosure or use of the information; . . . .”

52. The DTSA divides the term misappropriation into two categories: (1) improper acquisition and (2) improper use or disclosure.

53. The DTSA defines improper acquisition as the “acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means.”

54. Improper use or disclosure is defined as “disclosure or use of a trade secret of another without express or implied consent by a person who (a) used improper means to acquire knowledge of the trade secret; or (b) at the time of disclosure or use, knew or had reason to know that his/her knowledge of the trade secret was (i) derived from or through a person who had utilized improper means to acquire it; (ii) acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or (iii) derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; . . . .”

55. The DTSA defines “improper means” to include theft, bribery, misrepresentation, breach or inducement of a breach of duty to maintain secrecy, or espionage through electronic or other means.

56. While employed by Plaintiffs, Defendant obtained access to and misappropriated Plaintiffs’ trade secrets related to Plaintiffs’ products that are used in, or intended for use in, interstate or foreign commerce.

57. Plaintiffs consider the items misappropriated by Defendant to be valuable trade secrets, and they have taken reasonable steps as part of ongoing standard operating procedures to maintain the confidential nature of this information.

58. As a result of Defendant’s misappropriation and unauthorized use and removal of the confidential, proprietary and trade secret information described above, Defendant has violated the DTSA.

59. As a direct and proximate result of Defendant’s violations of the DTSA, Plaintiffs are likely to incur substantial damages as a result of Defendant’s misappropriation of trade secrets, in an amount that will be established at trial of this matter.



60. Defendant's actions in converting and misappropriating Plaintiffs' confidential, proprietary and trade secret information for his own gain were willful, wanton, and malicious, and were taken with reckless disregard for the rights of Plaintiffs.

61. Defendant's actions have caused and will continue to cause Plaintiffs irreparable harm if not preliminarily and permanently enjoined.

62. Plaintiffs have no adequate remedy at law.

WHEREFORE, Plaintiffs seek a judgment against Defendant for compensatory and exemplary damages, preliminary and permanent injunctive relief, prejudgment interest, an award of costs and reasonable attorneys' fees pursuant to the DTSA (18 U.S.C. § 1836(b)(3)(D)), and such other relief as the Court deems just and proper.

**COUNT II:  
VIOLATION OF THE MISSOURI UNIFORM TRADE SECRETS ACT**

63. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 62 as if fully alleged herein.

64. The Missouri Uniform Trade Secrets Act ("MUTSA"), Mo. Rev. Stat. §§ 417.450 to 417.467, provides injunctive relief for the actual or threatened misappropriation of trade secrets. *Id.* at § 417.455.

65. Under the MUTSA, Plaintiffs are also entitled to recover damages for the misappropriation of trade secrets, which can include both the actual loss caused by the misappropriation and the unjust enrichment caused by the misappropriation that is not taken into account in computing actual loss. *Id.* at § 417.457(1).

66. If the misappropriation is deemed outrageous because of the misappropriator's evil motive or reckless indifference to the rights of others, the Court may award punitive damages. *Id.* at § 417.457(2).

67. Based on Defendant's conduct described above, under the MUTSA, Plaintiffs are entitled to injunctive relief preventing Defendants from further using and/or disclosing Plaintiffs' trade secrets and requiring the return of Plaintiffs' trade secrets; damages, for an amount to be determined at trial, for the actual and/or threatened misappropriation of Plaintiffs' trade secrets; and punitive damages, for an amount to be determined at trial, based on Defendant's evil motive and/or reckless indifference to the rights of Plaintiffs.

WHEREFORE, Plaintiffs seek a judgment against Defendant for injunctive relief prohibiting Defendant from further disclosing and/or using Plaintiffs' trade secrets and requiring the return of Plaintiffs' trade secrets, actual and punitive damages against Defendant under the MUTSA, and such other relief as the Court deems just and proper.

**COUNT III:  
BREACH OF FIDUCIARY DUTY**

68. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 67 as if fully alleged herein.

69. As a valued employee entrusted with Plaintiffs' confidential business information, Defendant owed Plaintiffs a fiduciary duty of loyalty.

70. The conduct of Defendant described above, including the installation of sophisticated, unauthorized software on computers assigned to Defendant and theft of trade secrets on June 10, 2016, breached Defendant's fiduciary duty to Plaintiffs.

71. Defendant's conduct was intentional.

72. As a direct and proximate result of Defendant's breach of fiduciary duty, Plaintiffs are likely to incur substantial damages in an amount that will be established at trial of this matter.

WHEREFORE, Plaintiffs seek a judgment against Defendant for compensatory and punitive damages, prejudgment interest, and such other relief as the Court deems just and proper.

**COUNT IV:  
BREACH OF EMPLOYMENT AGREEMENT**

73. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 72 as if fully alleged herein.

74. There existed between Monsanto and Defendant an employment agreement that constitutes a valid employment contract, with offer and acceptance, and supported by consideration, which is attached hereto as Exhibit 1.

75. In his employment agreement with Monsanto, Defendant explicitly recognized and agreed he was given access to proprietary, highly valuable, and sensitive information, including trade secrets, and that he occupied a position of trust and confidence with respect to this proprietary information.

76. Defendant further agreed that he was to use his best efforts and diligence both during and after his employment with Monsanto to protect the confidential, trade secret, and /or proprietary character of all such information.

77. The conduct of Defendant described above, including the installation of sophisticated, unauthorized software on computers assigned to Defendant and theft of trade secrets on June 10, 2016, breached Defendant's employment agreement with Plaintiffs.

78. As a direct and proximate result of Defendant's breach of fiduciary duty, Plaintiffs are likely to incur substantial damages in an amount that will be established at trial of this matter.

WHEREFORE, Plaintiffs seek a judgment against Defendant for compensatory and punitive damages, prejudgment interest, and such other relief as the Court deems just and proper.

**COUNT V:  
CONVERSION**

79. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 78 as if fully alleged herein.

80. Plaintiffs are the rightful owner of the confidential and proprietary information taken on June 10, 2016.

81. Defendant is in wrongful possession of Plaintiffs' confidential and proprietary information.

82. Defendant has wrongfully taken possession with the intent to exercise some control over Plaintiffs' confidential and proprietary information in a manner inconsistent with Plaintiffs' ownership, entitlement to, and control of such information.

83. As a direct and proximate result of Defendant's conversion of Plaintiffs' confidential and proprietary information, Plaintiffs are likely to incur substantial damages in an amount that will be established at trial of this matter.

84. The value of Plaintiffs' confidential and proprietary information lies in its exclusive use by Plaintiffs and their employees. By wrongfully asserting dominion and control over this trade secret information, Defendant has diminished and threatens to further diminish its monetary value.

WHEREFORE, Plaintiffs seek a judgment against Defendant for compensatory and punitive damages, prejudgment interest, and such other relief as the Court deems just and proper.

**COUNT VI:  
REPLEVIN**

85. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 84 as if fully alleged herein.

86. Plaintiffs are the rightful owner of the confidential and proprietary information taken on June 10, 2016.

87. Defendant is in wrongful possession of Plaintiffs' confidential and proprietary information.

88. Defendant has wrongfully taken possession with the intent to exercise some control over Plaintiffs' confidential and proprietary information in a manner inconsistent with Plaintiffs' ownership, entitlement to, and control of such information.

89. As a direct and proximate result of Defendant's conversion of Plaintiffs' confidential and proprietary information, Plaintiffs are likely to incur substantial damages in an amount that will be established at trial of this matter.

90. The value of Plaintiffs' confidential and proprietary information lies in its exclusive use by Plaintiffs and their employees. Failing to return the confidential and proprietary information diminishes and threatens to further diminish its monetary value.

WHEREFORE, Plaintiffs seek a judgment against Defendant for compensatory and punitive damages, prejudgment interest, and such other relief as the Court deems just and proper.

**COUNT VII:  
VIOLATION OF THE MISSOURI COMPUTER  
DATA ACCESS AND FRAUD STATUTE**

91. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 90 as if fully alleged herein.

92. On at least June 10, 2016, Defendant knowingly and without authorization disclosed and took proprietary data, programs, and supporting documentation from the secure environment of Plaintiffs.

93. Defendant has received, retained, used, or disclosed this data in violation of R.S. Mo. § 569.095.

WHEREFORE, Plaintiffs seek a judgment against Defendant for compensatory and punitive damages, prejudgment interest, and such other relief as the Court deems just and proper.

### **CLAIMS FOR RELIEF**

WHEREFORE, Plaintiffs respectfully request this Court provide the following relief:

(A) An injunction prohibiting Defendant from further disclosing, transmitting, and/or using Plaintiffs' confidential trade secrets and requiring the return of Plaintiffs' confidential trade secrets;

(B) An order compelling Defendant to identify all cloud data storage accounts along with the user names and passwords for those accounts to allow Plaintiffs to recover its confidential business information and trade secrets misappropriated by Defendant and to conduct analytics on those accounts to determine whether additional transfers occurred.

(C) Actual damages in an amount to be determined at trial, to compensate Plaintiff for the actual loss caused by the wrongful disclosure and the misappropriation of its confidential trade secrets;

(D) Exemplary damages as provided for under the DTSA based on Defendant's willful and malicious actions;

(E) Punitive damages as provided for under the MUTSA based on Defendant's outrageous conduct; and

(F) Plaintiffs' attorneys' fees.

Respectfully submitted,

HUSCH BLACKWELL, LLP

/s/ Matthew T. Schelp

---

Matthew T. Schelp, 45724MO

Matthew P. Diehr, 61999MO

Mark C. Milton, 63101MO

190 Carondelet Plaza, Suite 600

St. Louis, MO 63105

T: 314.480.1500 / F: 314.480.1505

matthew.schelp@huschblackwell.com

matthew.diehr@huschblackwell.com

mark.milton@huschblackwell.com